PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/10, 19/00

A1

(11) International Publication Number: WO 00/49586

(43) International Publication Date: 24 August 2000 (24.08.00)

(21) International Application Number: PCT/IE00/00025

(22) International Filing Date: 18 February 2000 (18.02.00)

(30) Priority Data:

60/120,747	18 February 1999 (18.02.99)	US
60/129,033	13 April 1999 (13.04.99)	US
60/134,027	13 May 1999 (13.05.99)	US
60/144,875	20 July 1999 (20.07.99)	US
60/147,153	4 August 1999 (04.08.99)	US

(71) Applicant *(for all designated States except US)*: ORBIS PATENTS LIMITED [IE/IE]; 181 Howth Road, Dublin 3 (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FLITCROFT, Daniel, Ian [GB/IE]; 70 Lower Albert Road, Sandycove, County Dublin (IE). O'DONNELL, Graham [IE/IE]; 5 Lower Albert Road, Sandycove, Dun Laoghaire, County Dublin (IE).

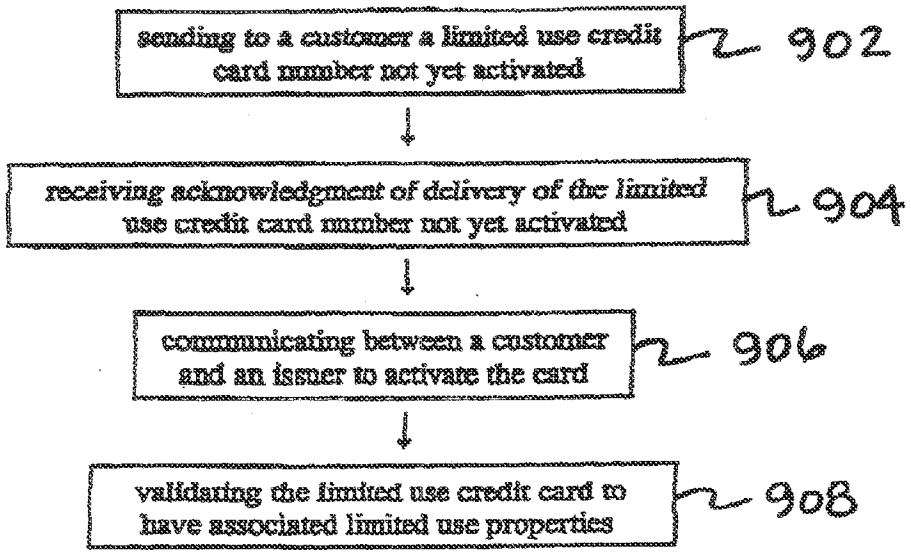
(74) Agents: O'CONNOR, Donal, H. et al.; Cruickshank & Co., 1 Holles Street, Dublin 2 (IE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DE (Utility model), DK, DK (Utility model), DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: CREDIT CARD SYSTEM AND METHOD



(57) Abstract

A credit card system is provided which has the added feature of providing additional limited use credit card numbers and/or cards. These numbers and/or cards can be used for a single or limited use transaction, thereby reducing the potential for fraudulent reuse of these numbers and/or cards. The credit card system finds application to "card remote" transactions such as by phone or Internet. Additionally, when a single use or limited use credit card is used for "card present" transactions, so called "skimming" fraud is eliminated. Various other features enhance the credit card system which will allow secure trade without the use of elaborate encryption techniques. Methods for limiting, distributing and using a limited use card nubmer, controlling the validity of a limited use credit card number, conducting a limited used credit card number transaction and providing remote access devices for accessing a limited use credit card number are also provided.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CREDIT CARD SYSTEM AND METHOD

Introduction

This invention relates to a credit card system and method, and more particularly, to a credit card system and method offering reduced potential of credit card number misuse.

The development of retail electronic commerce has been relatively slow in spite of the perceived demand for such trade. The single greatest deterrent to the expansion of retail electronic commerce is the potential for fraud. This potential for fraud has been a major concern for the credit card companies and financial institutions as well as the customers and the providers of the goods and services.

The former are concerned about fraud because essentially the financial institutions have to bear the initial cost of the fraud. Additionally, the credit card companies have an efficient credit card system which is working well for face to face transactions, i.e., "card present" transactions where the credit card is physically presented to a trader and the trader can obtain the credit card number, compare signatures and in many cases photographs before accepting a particular credit card.

The latter are equally concerned about fraud being well aware that ultimately the user must pay for the fraud. However, there are particular personal concerns for the consumer in that the fraudulent use of the credit card by misuse of the credit card number by a third party may not become apparent for some time. This can happen even if the card is still in his or her possession. Further, when fraud does occur the consumer has the task of persuading the credit card provider that fraud by another did indeed occur.

There is also the additional fear of being overcharged on a credit card. There are thus particular risks for those credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some considerable time before it is detected. One

particular form of fraud referred to as "skimming" is particularly difficult to control. What happens is that the card holder proffers his or her card at an establishment to make a transaction, the relevant information is electronically and/or physically copied from the card and the card is subsequently reproduced. This can be a particular problem with travelers particularly during an extensive period of travel as the fraudulent card may turn up in other places and it may be some considerable time before the fraud is detected.

For remote credit card use, the credit card holder has to provide details of name, master credit card number, expiration date and address and often many other pieces of information for verification; the storing and updating of the information is expensive but necessary. This of itself is a considerable security risk as anybody will appreciate that this information could be used to fraudulently charge goods and services to the card holder's credit card account. Such fraudulent use is not limited to those people to whom the credit card information has been given legitimately, but extends to anybody who can illegitimately obtain such details. A major problem in relation to this form of fraud is that the credit card may still be in the possession of the legitimate holder as these fraudulent transactions are taking place. This is often referred to as "compromised numbers" fraud. Indeed all this fraud needs is one dishonest staff member, for example in a shop, hotel or restaurant, to record the credit card number. It is thus not the same as card theft.

The current approaches to the limiting of credit card fraud are dependent on the theft of a card being reported and elaborate verification systems whereby altered patterns of use initiate some inquiry from the credit card company. Many users of credit cards have no doubt received telephone calls, when their use of the card has been exceptional, or otherwise unusual in the eyes of the organization providing the verification services.

Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, both in the general area of fraud for ordinary use of credit cards and for the particular problems associated with such remote use.

One of the developments is the provision of smart cards which are credit card devices containing embedded electronic circuitry that can either store information or perform computations. Generally speaking they contribute to credit card security systems by using some encryption system. A typical example of such a smart card is disclosed in U.S. Patent No. 5,317,636 (Vizcaino).

Another one of the developments is the Secure Electronic Transaction (SET) protocol which represents the collaboration between many leading computer companies and the credit card industry which is particularly related to electronic transmission of credit card details and in particular via the Internet. It provides a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction.

Another method that is particularly directed to the Internet is described in U.S. Patent No. 5,715,314 (Payne et al.). U.S. Patent 5,715,314 discloses using an access message that comprises a product identifier and an access message authenticator based on a cryptographic key. A buyer computer sends a payment message that identifies a particular product to a payment computer. The payment computer is programmed to receive the payment message, to create the access message, and to send the access message to a merchant computer. Because the access message is tied to a particular product and a particular merchant computer, the access message can not be generated until the user sends the payment message to the payment computer. Because the access message is different from existing credit card formats, the access message is ill-suited for phone/mail orders and other traditional credit card transactions.

U.S. Patent No. 5,883,810 (Franklin et al.) describes an online transaction system in which a user of the Internet or the like clicks on an icon to receive a proxy transaction number from a credit card provider. This proxy number stands in for the user's regular credit card number during transmission over the Internet, but expires after a short time (e.g., one hour) to reduce the chance that the number will be effectively intercepted

and fraudulently used. The processing that occurs when a bank receives transaction information from a merchant involves checking whether the proxy number is a valid number and whether the transaction value and merchant match. There is no additional processing triggered when the bank processing system receives the proxy number. In addition, a significant drawback of the Franklin et al. system is that an unscrupulous merchant or a criminal who is capable of accessing or intercepting order details can then turn around and use the proxy number a number of times before the lapse of the expiration term. Thus, more than one transaction can occur within the duration of the expiration term. The Franklin et al. system has nothing in place to prevent this type of fraud. The Franklin et al. system merely depends upon an assumption that fewer criminals could obtain the proxy number and reuse it within the expiration term of the proxy transaction number set by the issuing bank than the total number of criminals capable of gaining access to credit card numbers used for online commerce. Also, the inclusion of specific transaction information does not prevent a fraudulent merchant from recurrent unauthorized charges within the expiry time of the proxy number. The user will not be aware of this misuse of his/her credit card details until the receipt of the statement, which will typically not be until several weeks later.

There are also specific electronic transaction systems such as "Cyber Cash," "Check Free" and "First Virtual." Unfortunately, there are perceived problems with what has been proposed to date. Firstly, any form of reliance on encryption is a challenge to those who will then try to break it. The manner in which access has been gained to extremely sensitive information in Government premises would make anyone wary of any reliance on an encryption system. Secondly, a further problem is that some of the most secure forms of encryption system are not widely available due to government and other security requirements. Limiting the electronic trading systems and security systems for use to the Internet is of relatively little use. In addition, entirely new electronic payment systems require changes in how merchants handle transactions and this represents an important commercial disadvantage for such systems.

Additionally, various approaches have been taken to make "card present" transactions more attractive. For instance, Japanese Patent Publication No. Hei 6-282556

discloses a one time credit card settlement system for use by, e.g., teenage children of credit card holders. This system employs a credit card which can be used only once in which various information such as specific personal information, use conditions, and an approved credit limit identical to those of the original credit card are recorded on a data recording element and displayed on the face of the card. The one-time credit card contains the same member number, expiration date, card company code, and the like as on existing credit card, as well as one-time credit card expiration date not exceeding the expiration date of credit card, available credit limit for the card, and the like. The one-time credit card makes use of some of the same settlement means as the conventional credit card. However, the system also requires use permission information to be recorded on the credit card, the information permitting the credit card to be used only once or making it impossible to use the credit card when the credit limit has been exceeded. A special card terminal device checks the information taken from the card for correctness and imparts use permission information for when the card is not permitted to be used on the transmission to the credit card issuing company. The use permission information takes the form of a punched hole on the card itself. This system has obvious drawbacks, such as the card terminal having to be modified for additional functions (e.g., punching holes, detected punched holes, imparting additional information, etc.). Also, such a system offers little additional security insofar as fraud can still be practiced perhaps by covering the holes or otherwise replacing the permission use information on the credit card. Further, such a system would require a change in nearly all card terminal equipment if it were adopted.

Patent Nos. 5,627,355 and 5,478,994 (Rahman et al.) disclose another type of system that uses a plurality of pin numbers which are added to a credit card number on an electronic display. U.S. Patent No. 5,627,355 discloses a credit card having a memory element containing a series of passwords in a predetermined sequence. These passwords are identical to another sequence stored in a memory of a host control computer. Further, the card contains a first fixed field containing an account number (e.g., "444 222 333"). In operation, the memory element of the credit card device provides a unique password from the sequence with each use of the credit

card-device. This permits verification by comparing the account number and the password provided with each use of the device with the account number and the next number in sequence as indicated by the host computer. The host computer deactivates the password after the transaction. Among the drawbacks with this type of system is the need for a power supply, a display, a memory device, a sound generator and the need to recycle a limited sequence of pin numbers. Such a system is not readily adapted to current credit card transactions because it lacks the ability of providing a check sum of the card number and cannot be read by a standard card reader. Also, if the card is lost or stolen, there is little to prevent a person from using the card until it is reported to be lost or stolen by the correct holder. See, also, U.S. Patent No. 5,606,614 (Brady et al.).

Other attempts have been made to make funds available to an individual, but with limitations. For example, U.S. Patent Nos. 5,350,906 (Brody et al.) and 5,326,960 (Tannenbaum et al.) disclose issuing temporary PINs for one time or limited time and limited credit access to an account at an ATM. These patents disclose a currency transfer system and method for an ATM network. In this system, a main account holder (i.e., the sponsor) sets up a subaccount that can be accessed by a non-subscriber by presenting a fixed limit card associated with the subaccount and by entering a password corresponding to the subaccount. Once the fixed limit is reached, the card can no longer be used. The fixed limit card contains information on its magnetic stripe pertaining to the sponsor account.

One of the problems with all these systems is that there are many competing technologies and therefore there is a multiplicity of incompatible formats which will be a deterrent to both traders and consumers. Similarly, many of these systems require modifications of the technology used at the point of sale, which will require considerable investment and further limit the uptake of the systems.

Summary of the Invention

Many solutions have been proposed to the problem of security of credit card transactions. However, none of them allow the use of existing credit cards and existing credit card formats and terminal equipment. Ideally, as realized by the present inventors, the solution would be to obtain the functionality of a credit card, while never in fact revealing the master credit card number. Unfortunately, the only way to ensure that master credit card numbers cannot be used fraudulently is to never transmit the master credit card number by any direct route, i.e., phone, mail, Internet or even to print out the master credit card number during the transaction, such as is commonly the case at present.

According to exemplary embodiments of the present invention as described in the present inventor's earlier application (U.S. non-provisional application 09/235,836), a more secure way of using existing credit cards and, in particular, using existing credit cards in remote credit card transactions was provided. The present invention is further directed towards providing a more secure way of using existing credit cards generally which will not require any major modifications to existing credit card systems. It is further directed towards providing a credit card system that will be user friendly and will provide customers with a greater confidence in the security of the system.

These and other advantages of the present invention are satisfied by a first exemplary embodiment, which pertains to a method used in a financial transaction system capable of using a limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of said at least one credit card number and which is associated the master account number of a customer. The method controls the validity of the limited use credit card number and includes the steps of: sending to a customer from a limited use credit card number issuer a limited use credit card number which is not yet activated; receiving acknowledgment of delivery by the customer of the limited use credit card number which is not yet activated; communicating with a limited use card number card issuer to activate the

card before it can be used in a transaction; and validating the limited use credit card to have associated limited use properties. These properties can be such things as a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

The validation step can include activating validity limited credit card software using a user identification to identify the user with the card issuer; requesting validation of a limited use credit card for a merchant as identified by a merchant identification number; and providing an option for a user to specify additional limitations other than the specific merchant to the limitation on the limited use credit card number.

Additionally, the present invention provides a method of conducting a limited use credit card transaction, which includes initiating a transaction by a customer presenting a limited use credit card number to a merchant; routing said limited use credit card number to a central processing system; determining whether said limited use credit card number has been deactivated because the limited use condition has been satisfied; transmitting a signal to the merchant denying authorization of the card number if the credit card number has been deactivated; transmitting a signal to a master credit card issuing facility which issued that limited use credit card number, said signal including original transaction details but with the limited use credit card number remapped to be a master credit card number if said limited use credit card number has not been deactivated; determining at the whether authorization can be obtained against the master credit card number; authorizing or denying authorization of the transaction based on this determination; remapped any such authorization or denial to the limited use credit card number for transmission to the merchant; and transmitting a signal to the merchant authorizing or denying authorization of the limited use credit card number.

Further, the present invention provides a method of conducting a settlement transaction including transmitting a signal from a merchant to a central processing system according to a BIN of the limited use card number; remapping the limited use credit card number with the master credit card number; transmitting said remapped

master credit card number to issuer processing facility which issued the master credit card number; settling the transaction by payment, if appropriate, to the central processing system; remapping the master credit card number back to the limited use credit card number; and transmitting the limited use credit card number and payment information, if appropriate, to the merchant.

Furthermore, the present invention includes a method of providing remote access devices for accessing limited use numbers. The method includes submitting user authentication information and the master account number for entry into a database; determining whether the user is a valid user of the master credit card number; registering the user if the user is determined to be a valid user; obtaining by registered users a software package to which enables communication with a remote access device support server to enable the issuance of limited use card numbers; using the software package to initiates communication with the remote access support server; authenticating the user at the remote access support server; requesting a limited use number by an authenticated user; specifying by the authenticated user any additional transaction limitations desired; obtaining an available limited use number; entering the limited use number and the specified limitations into the database such that the limited use number is associated with the user's information already in database; and transmitting the limited use number to the user.

In this way, a merchant can receive a limited use credit card number; process the received limited use credit card number in a transaction as any other credit card number; pass the transaction through to the card issuer's processing system; and request authorization of the transaction at the card issuer's processing system against the associated limited use properties. The system can then deactivate the limited use credit card number by the card issuer when a use-triggered condition is present. Also, limited use transaction numbers can be obtained by authorized users and transactions can be processed within the existing credit card system with only minor modifications.

DETAILED DESCRIPTION OF THE INVENTION

The present invention will be more readily understood upon reading the following detailed description in conjunction with the drawings in which:

Fig. 1 shows an exemplary system for implementing the present invention;

Fig. 2 shows, in high-level form, the operation of the central processing station shown in Fig. 1;

Fig. 3 is a flow chart illustrating an exemplary process for allocating credit card numbers;

Fig. 4 is a flow chart illustrating an exemplary process for limiting the use of a credit card number;

Fig. 5 is a flow chart illustrating an exemplary process for distributing credit card numbers;

Fig. 6 is a flow chart illustrating an exemplary process for electronically using credit card numbers;

Fig. 7 is a flow chart illustrating an exemplary process for processing a transaction;

Fig. 8 is a flow chart illustrating another exemplary process for processing a transaction;

Fig. 9 is a flow chart illustrating an exemplary method of controlling the validity of a limited use credit card number;

Fig. 10 is a flow chart illustrating an exemplary process for using a credit card

— number as a PIN number;

Fig. 11 is a block diagram illustrating an exemplary location for the central processing system;

Fig. 12 is a flow chart illustrating an exemplary method of conducting a limited use credit card number transaction;

Fig. 13 is a flow chart illustrating an exemplary method of conducting a settlement transaction;

Fig. 14 is a block diagram illustrating an alternate exemplary location for the central processing system;

Fig. 15 is a block diagram illustrating an alternate exemplary process for limiting, distributing and using a limited use card number; and

Fig. 16 is a flow chart illustrating an exemplary method of providing remote access devices for accessing limited use credit card numbers.

In this specification the term "credit card" refers to credit cards (MasterCard®, Visa®, Diners Club®, etc.) as well as charge cards (e.g., American Express®, some department store cards), debit cards such as usable at ATMs and many other locations or that are associated with a particular account, and hybrids thereof (e.g., extended payment American Express®, bank debit cards with the Visa® logo, etc.). Also, the terms "master credit card number" and "master credit card" refer to the credit card number and the credit card as generally understood, namely, that which is allocated by the credit card provider to the customer for his or her account. It will be appreciated that an account may have many master credit cards in the sense of this specification. For example, a corporation may provide many of its employees with credit cards but essentially each of these employees holds a master credit card even if there is only one customer account. Each of these master credit cards will have a

unique master credit card number, which set of master credit card numbers will be linked to the account. Similarly, in families, various members of the family may hold a master credit card, all of which are paid for out of the one customer account.

Additionally, the "master credit card" account can be in some embodiments something other than a credit card account. For instance, while not otherwise affecting the formatting or processing of the limited use credit card numbers as described herein, the master card number can be a prepaid account or another type of account, such as a utility, telephone service provider or Internet Service Provider (ISP) account. The utility company, telephone company, ISP or other account holder would generate a bill, which, in possible addition to or separate from to the regular bill, would include a listing of limited use credit card transactions. An advantage of this type of arrangement is that the service provider already has information as to a pool of individual and their credit worthiness, as well as low increased overhead due to the already in place billing system. In these embodiments, the "master account" may but likely does not have the format of a standard credit card or the like.

The term "limited-use" credit card number is used to encompass at least both the embodiment in which the credit card is designated for a single use, and the embodiment in which the credit card is designated for multiple uses providing that the charges accrued do not exceed a prescribed threshold or thresholds, such a total single charge, total charges over a limited time period, total charge in a single transaction, etc. A common feature is that the limitation is based on a use-triggered condition subsequent, and not just the expiration date of the card. Stated differently, the a limited-use credit card number is deactivated upon a use-triggered condition which occurs subsequent to assignment of said at least one credit card number.

The terms "card holder" and "user" are used interchangeably to refer to an entity, e.g., an individual, that has been rightfully issued a credit/debit/charge card number, e.g., through a contractual arrangement, or that has been authorized to use such card by such entity or a representative of such entity.

There are at least two basic different ways of carrying out the present invention. In summary, they are the allocation of additional credit card numbers for remote trade and secondly the provision of what are effectively disposable credit cards for remote and card present trade, both of which have the feature of in the case of single use or in the case of multiple use, protecting against the worst effects of compromised numbers fraud or skimming.

In a refinement of the invention, it is possible to control the manner in which an actual transaction is carried out as a further protection against unscrupulous providers of goods and services.

Essentially, there are certain matters that will be considered in relation to this invention. They are firstly the operational or functional features in so far as they affect customers, and then there are the technical features, namely how the invention is implemented, how the invention is provided to the customers, and finally, how the invention is handled by the providers of goods and services and the processors of the credit cards, i.e., the financial institutions and/or their service providers.
The operational or functional features of this invention will be discussed first in the context of a standard credit card system.

One basic feature of the invention is to provide in a credit card system such that each master credit card holder could be provided with one or more of the following: 1) additional single use credit card numbers for remote transactions; 2) multiple use credit card numbers for remote transactions; 3) single use additional credit cards for remote and card present transactions; and 4) multiple use credit cards for remote and card present transactions.

It is also envisaged that in certain situations credit cards can be provided to people who do not have an account with any credit card company. This latter feature is described in more detail below. Various other features may be provided in the above situations, which will further improve the security of credit card transactions.

Dealing firstly with the situation where a master credit card holder has an additional credit card number allocated to him or her for a single use, it will be appreciated that since the number can only be used for one single transaction, the fact that the number is in anybody else's hands is irrelevant as it has been deactivated and the master credit card number is not revealed to the third party. Various other features may be added to such single use credit card numbers, for example, the value of the transaction can be limited, thus the master credit card holder can have a plurality of single use credit card numbers of differing values. For example, when a remote trade is carried out, the master credit card holder will use a credit card number which has a credit card limit only marginally above or equal to that of the value of the transaction. This would reduce the chances of or prevent an unscrupulous trader using the credit card number to supply additional goods or services over those ordered or to increase the agreed charge.

A second embodiment of the invention provides the master credit card holder with an additional credit card number for use in remote trade, which credit card number could have, as in the previous example of the invention, a credit limit for each specific transaction or a credit limit such that when the aggregate amount of a series of transactions exceeded a specific credit limit that the credit card number would be canceled, invalidated or in some other way deactivated. Similarly, the multiple use credit card number could be limited to, for example, five uses with a credit limit not exceeding $100 in each transaction and an aggregate credit limit not exceeding $400. Similarly, a time restriction could be put on such a credit card number in that it would be deactivated if it was used with frequency above (or below) a given threshold, for example, more than once a week. It will be appreciated that the limits that can be placed on the use of a single use credit number or a multiple use credit card number are almost limitless and those having skill in the art will consider other ways in which the use of the credit card number could be limited, whether it be by time, by amount, frequency of use, by geographical region, by merchant, by merchant class, or by purpose or use (such as limited to Internet trade and so on), or by some combination of these separate criterion.

The third way in which the invention could be carried out is by physically providing additional single use credit cards each of which would have a unique additional credit card number. Such additional single use credit cards could then be used both for remote trade by using the additional credit card numbers for respective transactions, and for "card present" trade where each card would be "swiped" in the normal manner. Such a disposable credit card could be made like any common credit card, or from a relatively inexpensive material, such as cardboard or thin plastic, with the relevant information entered into it in readable (e.g., magnetic) form, as is already the case with many forms of passes for use in public transport and the like. Again, substantially the same features as with the credit card number could be provided. Thus, for example, the disposable credit card could be limited to use geographically, to a use, to an amount, to a frequency of use, to an expiration date, and so on. Again, those skilled in the art will appreciate that there are many variations to this concept.

Another way of carrying out the invention is to provide a master credit card holder with a multiple use additional credit card, where the additional credit card provides any limitations as to use triggered conditions subsequent that may be desired.

Ideally, irrespective of the manner in which the invention is carried out, the master credit card holder would be provided with either a plurality of single use additional credit card numbers or multiple use credit card numbers or a mixture of single and multiple use credits cards.

It will be appreciated that with either single use credit card numbers or single use additional credit cards, it is possible to eliminate or reduce the risk of credit card number fraud. Further, depending on the credit limit imparted to the particular credit card number or additional credit card number or single use additional credit card, it is possible to further limit the possibilities of fraud in any remote transaction and that with the use of a disposable single use credit card it is possible to eliminate or reduce the risk of skimming.

With multiple use additional credit card numbers and multiple use additional credit cards, the above-identified problems may not be totally eliminated due to preferences of the user. This is because, in certain circumstances, credit card users may prefer to have, for example, an additional credit card number for remote trade with a specific credit limit that they use all the time and are willing to take the risk of compromised number fraud, in the sense that they can control the severity of this misuse. This would be particularly the case where some of the various user triggered conditions subsequent limitations suggested above are used with the additional credit card number. Substantially the same criteria would apply to an additional multiple use credit card.

Effectively, the present invention solves the problem by obtaining the functionality of a credit card while never in fact revealing the master credit card number as the master credit card number need never be given in a remote transaction. Further, the master credit card itself need never be given to a trader.

In another embodiment of the invention, it is envisaged that people who do not hold master credit cards could purchase disposable credit cards which would have a credit limit for the total purchases thereon equal to the amount for which the credit card was purchased. These could then be used for both card present and card remote trade, the only proviso being that if the credit limit was not reached it will then be necessary for a refund to be given by the financial institution or credit card provider. An obvious way of obtaining such a refund would be through an automatic teller machine (ATM). In this way, the existing credit card transaction system is employed and the card holder is given the convenience of having a credit card.

As an alternative, the above-discussed cards could be, in effect, debit cards in the true sense, in which funds are withdrawn against a customer's account. In this case, the "credit card" issued, whether it be a one time use card or multi-use card, and whether have a credit limit or not, would be used to debit the account immediately. Preferably, the credit card issued in these circumstances would be single use with or without a transaction amount limit which would be used and processed by the

customer and merchant for a transaction as if it were a credit card, while in the customer's bank it would be treated like any other debit to the account.

Various aspects of the invention may be embodied in a general purpose digital computer that is running a program or program segments originating from a computer readable or usable medium, such medium including but not limited to magnetic storage media (e.g., ROMs, floppy disks, hard disks, etc.), optically readable media (e.g., CD-ROMs, DVDs, etc.) and carrier waves (e.g., transmissions over the Internet). A functional program, code and code segments, used to implement the present invention can be derived by a skilled computer programmer from the description of the invention contained herein.

Fig. 1 shows an exemplary overview of a system for implementing the limited use credit card system of the present invention. The system 100 comprises a central processing station 102, which, accordingly to exemplary embodiments, may be operated by the credit card provider. Generally, this station 102 receives and processes remotely generated credit card transactions. The credit card transactions can originate from a merchant in the conventional manner, e.g., by swiping a credit card through a card swipe unit 106. Alternatively, the credit card transaction requests can originate from any remote electronic (e.g., a personal computer) device 104. These remote devices can interface with the central processing station 102 through any type of network, including any type of public or propriety networks, or some combination thereof. For instance, the personal computer 104 interfaces with the central processing station 102 via the Internet 112. Actually, there may be one or more merchant computer devices (not shown) which receive credit card transactions from the remote electronic device 104, and then forward these requests to the central processing station 102. The central processing station 102 can also interface with other types of remote devices, such as a wireless (e.g., cellular telephone) device 140, via radiocommunication using transmitting/receiving antenna 138.

The central processing station 102 itself may include a central processing unit 120, which interfaces with the remote units via network I/O unit 118. The central

processing unit 120 has access to a database of credit card numbers 124, a subset 126 of which are designated as being available for limited use (referred to as the "available range"). Also, the central processing unit 120 has access to a central database 122, referred to as a "conditions" database. This database is a general purpose database which stores information regarding customers' accounts, such as information regarding various conditions which apply to each customers' account. Further, this database 122 may store the mapping between a customer's fixed master credit card number and any outstanding associated limited use credit cards, using, for instance, some type of linked-list mechanism. Databases 122 and 124 are shown separately only to illustrate the type of information which may be maintained by the central processing station 102; the information in these databases can be commingled in a common database in a manner well understood by those having skill in the data processing arts. For instance, each limited use credit card number can be stored with a field, which identifies its master account, and various conditions regarding its use.

The central processing unit 120 can internally perform the approval and denial of credit card transaction requests by making reference to credit history information and other information in the conventional manner. Alternatively, this function can be delegated to a separate clearance processing facility (not shown).

Finally, the central processing station includes the capability of transmitting the limited use credit card numbers to customers. In a first embodiment, a local card dispenser 128 can be employed to generate a plurality of limited use cards 132 and/or a master credit card 134 for delivery to a customer. In a second embodiment, the limited use credit card numbers can be printed on a form 136 by printer 130, which is then delivered to the customer via the mail. The printed form 136 may include material which covers the numbers until scratched off, thereby indicating what numbers have been used and are no longer active. This listing of numbers can be included in a monthly or other periodic account statement sent to the customer. In a third embodiment, these limited use numbers can be electronically downloaded to a user's personal computer 104, where they are stored in local memory 142 of the personal computer 104 for subsequent use. In this case, the credit card numbers can be

encrypted (described in detail later). Instead of the personal computer 104, the numbers can be downloaded to a user's smart card though an appropriate interface. In a fourth embodiment, the single-use credit card numbers can be downloaded to a radio unit 140 (such as a portable telephone) via wireless communication. In a fifth embodiment, an ATM 108 can be used to dispense the limited use cards 110. Those skilled in the art will readily appreciate that other means for conveying the numbers/cards can be employed. These embodiments are, of course, usable together.

The logic used to perform the actual allocation and deactivation of limited use credit card numbers preferably comprises a microprocessor, which implements a stored program within the central processing unit 120. Any general or special purpose computer will suffice. In alternative embodiments, the logic used to perform the allocation and deactivation of the limited use credit card numbers may comprise discrete logic components, or some combination of discrete logic components and computer-implemented control.

Fig. 2 shows a high-level depiction of the functions performed by the central processing station 102 or the like. The process begins in step 202 by allocating one or more limited use numbers to a customer. These numbers are ultimately selected from the list 126 of available limited use numbers, or some other sub-set-list which has been previously formed from the numbers in list 126. Also, although not shown in Fig. 2, a master account number would have been preferably assigned to the customer at a previous point in time. The conditions database 122 may comprise a mechanism for associating the master account number (which can be a credit card number or some other type of account) number with the limited use credit card number. Because the limited use cards are arbitrarily chosen from the listing 126 of limited use card numbers, there should be no discernable link which would allow anyone to determine the master credit card number from any of the limited use numbers.

The processing then advances to step 204, where it is determined whether a customer requests or an event triggers a request for additional limited use cards or

card numbers. If so, additional limited use cards or card numbers are allocated to the customer.

Processing then advances to step 206, where the central processing station determines whether a transaction has taken place using a previously issued limited use card. This step is followed by a determination (in step 208) whether the limited use number should be deactivated. For instance, if the card is a single-use card, it will be deactivated. If the card is a fixed-limit card, the card is only deactivated if the recent transaction exceeds some stored threshold limit. These threshold limits can be stored on the card itself or in the conditions database 122. The actual step of deactivating is performed by generating a deactivation command, as represented in step 210 shown in Fig. 2. Naturally, there are other steps to processing a credit card transaction, such as checking whether the card is deactivated or otherwise invalid prior to completing the transaction. These additional steps are system specific and are not discussed here for sake of brevity.

Once a number is deactivated, this number can not be fraudulently reused. Hence, the risk of fraudulent capture of these numbers over the Internet (or via other transmission means) effectively disappears. In an alternative embodiment of the invention, these deactivated numbers can be reactivated providing that a sufficiently long time since their first activation has transpired. Providing that there is a sufficiently large number of limited use credit card numbers to choose from, it would be possible to wait a long time before it was necessary to repeat any numbers. At this point, it would be very unlikely that someone who had wrongfully intercepted a credit card number years ago would be motivated to fraudulently use it before the rightful owner.

After the limited use card is deactivated or a number of limited use cards are deactivated, an additional limited use card or cards can be activated. As described in detail in the following section, the actual activation of the credit card number can involve various intermediate processing steps. For instance, the credit card numbers from the list 126 can be first allocated to an "allocated" range of numbers, and then to an "issued but not valid" range of numbers, and then finally to an "issued and valid"